

From Bathroom Restrictions to “Algorithmic Cruelty”: Employer Surveillance in the Digital Age and its Manifestations in the Indian State

By: Namrata Raju¹ and Chitra Rawat¹

¹Independent Researcher

Keywords: surveillance, monitoring, digital Taylorism, surveillance capital

Abstract

This article explores the issue of employer surveillance in the global context and how extant employer-worker power imbalances are heightened in the digital age. While conversations on the “fourth industrial revolution” archetypally focus on Global North contexts, this article explores implications in the Indian state, which has a labour force primarily comprised of informal workers. The piece examines how employers are attempting to frame surveillance in less threatening ways but simultaneously engage in intrusive data capture from workers. It then delves into the different ways employer surveillance manifests across different sectors in the Indian context. The piece finally explores ways in which the issue of employer surveillance of workers in an era of “surveillance capitalism” can be countered in practical ways that center worker interests, rights, and welfare.

“They stalk you by scanner. Every single thing you do, you are being watched!”

- Interview with an American Amazon Warehouse Picker, extracted from a UNIGlobal Union report

Introduction

In a 2021 report aptly titled, *The Amazon Panopticon*ⁱ, UNIGlobal Union documents the myriad ways in which Amazon surveils its workers. The report observes that the tech giant deploys an array of digital tools to surveil its staff, with additional plans in the pipeline to utilize future technological innovations towards the same ends. The report notes, “Amazon is investing heavily in technological development to tighten its grip on workers by expanding its digital panopticon: patents it owns reveal the company’s plans to introduce new surveillance technologies, from augmented reality goggles to digital wristbands that track employees’ movements.” (UNIGlobal, 2021). The report presents several examples of the miscellaneous ways via which workers face exploitation, including the use of technology to monitor workers in excess, sometimes to the extent that workers are fearful of even taking bathroom breaks. Amazon Delivery drivers were documented as having to relieve themselves in plastic bottles out of fear of reprisal if they were to take a bathroom break when out for a delivery (UNIGlobal, 2021).

With the evolution of new technologies and employers’ easy access to these digital tools, workers around the world, particularly those living with varying forms of employment precarity, have been rendered severely vulnerable to exploitation through heightened employer surveillance. Despite these dire circumstances, the phrases “Digital Revolution,” the “Second Machine Age,” and “Fourth Industrial Revolution” are put to ubiquitous use by industry and governments around the world. Subsequently, these phrases are typically framed

as solutions to global problems or harbingers of a promising future (Gray and Suri, 2019). Workers are often a blind spot to this framing of technology being revolutionary: frequently jettisoned is the extant power imbalance between workers and employers, already acute but further heightened by the misuse of digital tools by employers within ever-evolving global labour markets.

The issue of employer surveillance, however, has long existed in numerous ways and has been heightened by the evolution of digital tools and technologies. These have also resulted in altering traditional labour relations (Athreya, 2020). This has rendered workers even more precarious than in prior decades. In a world where systems are driven by the interests of big capital as opposed to those of workers, it is not the technology itself that is inherently the problem. Rather, it is the constant evolution of labour markets to cater to the interests of big capital, which in our current techno-centric world, scholar Shoshana Zuboff titles, “surveillance capital.” In her 2019 book, *The Age of Surveillance Capitalism*, Zuboff observes,

“We are not alone in falling prey to the technology illusion. It is an enduring theme of social thought, as old as the Trojan horse. Despite this, each generation stumbles into the quicksand of forgetting that technology is an expression of other interests. In modern times, this means the interests of capital, and in our time, it is surveillance capital that commands the digital milieu and directs our trajectory towards the future.” (Zuboff, 2023)

In the realm of Big Tech, many argue that there is a close relationship between capital, tech, and surveillance: rights groups (Amnesty International, 2024) and experts alike have long raised concerns that this era of “surveillance capitalism” necessitates stringent law, policy, and governance frameworks surrounding data privacy (Harper, 2023). The above holds true for workers and consumers alike.

These concerns are further exacerbated in markets that have additional complications, such as the high degree of workforce informality in several emerging market economies worldwide. Often, discussions on the “future of work,” which investigate the interplay between labour markets and technology, focus on formal labour markets as opposed to the predicament of workers in developing nations (Athreya, 2020). This necessitates a closer investigation of the question of employer surveillance in emerging markets. In the Indian case, for instance, most of the country’s workforce is informal. Its tech industry makes for an interesting example since Indian tech is inextricably linked with the American tech sector: layoff cycles in the latter or contractions in the market often have spillover implications for India (Raju, 2023). The following sections investigate the question of technology and employer surveillance. These issues have first been raised in a global context, owing to the international nature of industries such as Big Tech, as well as the transnational nature of big capital. The piece then examines the different manifestations of employer surveillance in the Indian context. It concludes with the key practical considerations that must be weighed if worker interests are to be safeguarded, their rights ensured, and their privacy protected.

Employers Repackage Surveillance as “Staff Monitoring” for Palatability

Upon examining global trends in workplace surveillance by employers, it is imperative to note that they customarily look at “worker monitoring” and “worker surveillance” as synonymous. The term “monitoring” is often deployed by employers across multiple sectors worldwide as a more anodyne phrase that can be utilized: frequently a labour-washing effort, masking grave and repeated infractions into worker privacy. The business of spying on workers to heighten productivity, often at the risk of violating labour rights and other human rights in the workplace, has also bred a booming global industry. Several online services, for example, frame these “monitoring” services as part of a bouquet of human resource products to improve a company’s Return on Investment (ROI) from its employees (Empmonitor, 2024). Exacerbating this issue is the habitually missing lens upon worker needs: worker representation via trade unions. These may often be absent from employer considerations. Sometimes, even in the event of worker concerns being included, employers utilize the labour-washing language of “employee feedback” or co-opt employee committees to ultimately serve their own interests.

This anodyne framing of “employee monitoring” often runs counter to the deeply insidious nature of the information collected by employers, raising the overarching question of where monitoring ends and surveillance begins in labour markets worldwide. Several tech companies have now taken to using software such as *HubStaff*, *Time Doctor*, *Effiwork*, and *Insightful*, all of which brand themselves as “employee monitoring” and “employee productivity” tools. Worker monitoring has long been a child of productivity tracking by employers, gaining impetus during the Industrial Revolution with the burgeoning of simple tools such as the punching of attendance cards in factories. Over time, with the ratification of management technologies, worker monitoring has since expanded to include intrusive ways of collecting workers’ behavioral information, even expanding monitoring activities to include non-work related activities. (Eurofound, 2020).

In addition to tracking workers’ attendance, employers engage in different types of worker surveillance, which are often conveniently presented under the guise of employee monitoring. These include remote monitoring and time tracking, gamification and algorithmic management, prediction and flagging tools, and even biometric and health data (Mateescu and Nguyen, 2019). Figure 1 below details the different types of “monitoring” that workers across sectors and job types around the world may experience from the start to the close of an average work day.

The gamification of the workplace has precipitated a shift away from traditional labour relations, with platform companies, in particular, disrupting these relations through “digital labour arbitrage” (Athreya, 2020). Gamification of work refers to the integration of game-design elements to increase worker performance by implementing reward systems like scoreboards and badges that can be tied to monetary or non-monetary incentives. The case of platform companies raises some pressing concerns. Upon dividing tasks into several micro-tasks named “gigs” over which employers proceed to exert surveillance, platforms engage in micro-negotiations with workers. The shift in labour relations hence arises from dividing traditional wage labour into multiple smaller segments, with the employer ensuring that they exercise control over every worker for each minute segment (Empmonitor, 2024). Further confounding this issue of excessive employer control over every worker’s action is the

concern of increased management not by people but by algorithms instead. “Algorithmic management” often utilizes Taylorism (Munich Business School), the idea of breaking down tasks into smaller pieces for the purpose of productivity, and synergizes with artificial intelligence to collect data on workers and surveil them at every minuscule stage (Athreya, 2020). The lack of people behind making management decisions in the process of “Algorithmic management” often translates into “Algorithmic cruelty” for workers. A term invented by a web design consultant named Eric Meyer in 2014, “inadvertent algorithmic cruelty,” describes the lack of empathy that stems from a flaw in computational design (Gray and Suri, 2019). The above then translates into workers often facing unfair, and what is essentially illegal, wage deductions even for errors entirely outside of their control and purview, for which they should not be penalized (UNIGlobal, 2021).

Figure 1- Different Types of Surveillance (“Monitoring”) During a Day of Work

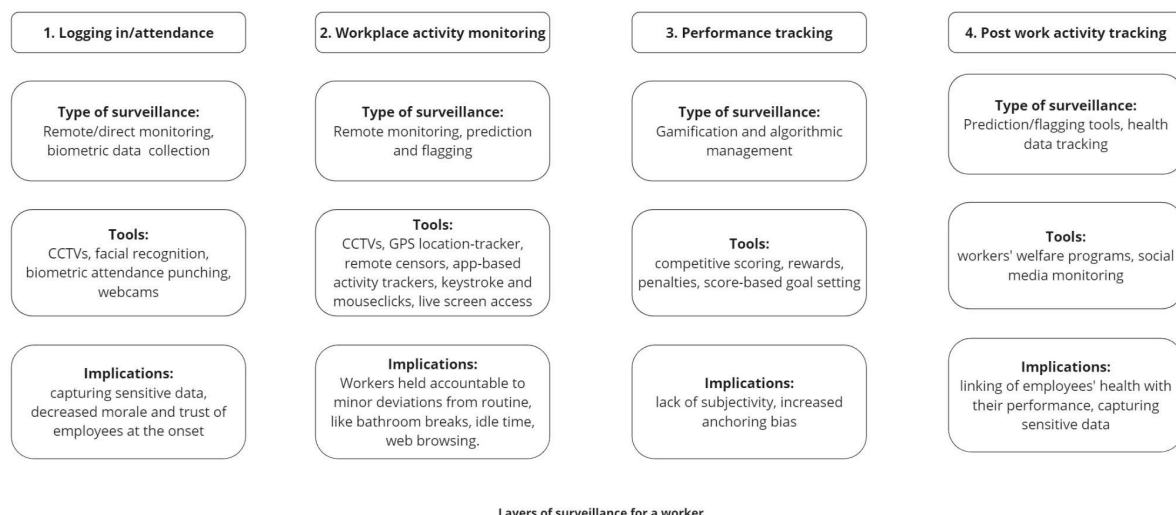


Image Source: Developed by Namrata Raju and Chitra Rawat (Based on a literature review)

1) Employer Surveillance: The Indian Context

Rather than viewing surveillance as a technology that has social consequences, it is essential to approach it as a social and political process with technological consequences in order to understand the implications for workers (Clavell, 2011). It is owing to this reason that surveillance tools are not uniform across sectors, as employers tend to adopt surveillance techniques contingent upon the utility they serve and the larger context of the workplace. Garment factories, for instance, often employ CCTV cameras as a surveillance “panopticon,” monitoring workers to “enforce discipline” and as a supposed deterrent to pilferage and theft. Conversely, in big tech companies, facial recognition techniques are often used to track attendance as a replacement for the more standard timesheet from preceding decades. In this regard, India is not dissimilar to global trends in employer surveillance methods.

Employer surveillance practices in the Indian context vary based on the nature of employment, together with the type of industry, ranging from basic tools like CCTV cameras to advanced surveillance such as AI-based facial recognition systems. What does set India apart, however, is the composition of its workforce relative to countries, especially in the

Global North, with more formalized workforces. The surveillance of workers is also not restricted to the realm of the private sector and businesses alone. In the informal sectorⁱⁱ, which forms 93% of the total workforce in the country and employs large volumes of migrant workers (NCEUS, 2009), workers often face state-sanctioned surveillance as well, owing to requirements such as destination-specific identity cards and residence proof requirements (Mukherjee, Piu; Bino, Paul G D; Pathan, 2013; Prasad-Aleyamma, 2018). Employers are often compelled to comply with these state-sponsored rules, as seen in Kerala's potential mandate for police clearance certificates for interstate migrant workers, in a state where almost 89.4% of employers collect the identification details of workers (Kerala Institute of Labour and Employment, 2020; T, 2023). The remainder of this section investigates the different types of employer surveillance methods in India, how these vary across industries, the links between a worker's degree/ type of marginalization, and how this marginalization renders them vulnerable to abuse via surveillance.

Workers' Surveillance at the Intersection of Vulnerability and Marginalisation

The Business Process Outsourcing (BPO) sector has a long history of employee monitoring, where all worker activities are recorded with the supposed aim of adhering to quality assurance and quality control metrics. The intersectional nature of worker vulnerabilities and their exposure to exploitation is also apparent with BPOs: it is characteristically more junior white-collar workers that are monitored. In recent years, we have witnessed tighter monitoring of BPO employees. AI facial recognition for attendance tracking has become more commonplace, with automated nudges being sent to workers even with the advent of their voice tones changing (Mateescu and Nguyen, 2019). This excessive surveillance places additional cognitive burdens upon workers, typically with no mechanisms available for relief, especially in the form of fully active worker unions. Furthermore, workers typically have little control over contesting algorithmic management decisions in the Indian context: quintessential "algorithmic cruelty," as observed in previous sections. In the BPO sector, worker monitoring software ranges from productivity and time trackers to even the recording of all worker conversations.

The specific hue of workers' intersectional vulnerabilities often manifests in the precise way they experience exploitation in the workplace; this is also true of surveillance. Given this context, it is vital to underscore that in India, most informal work is performed by workers from marginalized communities, which includes women workers, workers from lower castes (Dalits and Other Backward Classes), and tribal/Indigenous individuals - administratively termed as the Scheduled Castes and Scheduled Tribes respectively. The inherent nature of surveillance thus takes on various insidious guises as it intersects with workers from different types of marginalized backgrounds. Reports indicate that female workers, for example, are more likely to be subjected to surveillance in India (Sahni, 2023). The surveillance of sanitation workers makes for another instance since workers in sanitation tend to hail predominantly from lower-caste groups, implying that most Dalit women will likely face particularly egregious and excessive types of surveillance (National Campaign on Dalit Human Rights) (Sardar, 2023).

In a 2020 paper, Eckstein and Mawii illustrate how low-paid workers under contractual employment are susceptible to employers' monitoring efforts, which exacerbates their workplace precarity (Eckstein. and Mawii, 2020). Similarly, in the case of gig economy workers, information from workstations and work devices is often intercepted by employers

without the knowledge of workers. This is because contracts or other agreements may be orchestrated in a way to deliberately obfuscate language and apps designed to allow for overriding worker consent even upon being downloaded. During the pandemic, the Indian Federation of App-based Transport Workers (IFAT) raised this issue of opacity around data sharing between platform apps and India's government-mandated COVID tracing app, Aarogya Setu, after the download of the latter was made compulsory. In addition to this, workers are unaware of where their data is going, as exemplified by the case of ASHAⁱⁱⁱ workers forced to download the application during COVID (Internet Freedom Foundation). The COVID-19 pandemic further accelerated the demand for employee monitoring software, especially with work-from-home (WFH) protocols and increased reports of moonlighting. This was true around the world, and it was similar to the case of India. The formal sector was already equipped with advanced surveillance systems like time-tracking and biometric attendance. The pandemic, however, saw a surge in remote monitoring tools, such as the live webcam and live screen tracking devices, which were additionally equipped with features like browser history tracking and keystroke/mouse click monitoring. With the demand for such surveillance technologies spiking in information technology (IT), fast-moving consumer goods (FMCG), banking, financial services, and insurance (BFSI), and other tech-focused industries, companies that offer monitoring services like *TrackOlap* and *EmpMonitor* have almost doubled their growth rates in a single year (Sahu, 2023).

In industries such as garment manufacturing, however, where different parts of the supply chain lie within both the organized and unorganized sectors, surveillance is not as technologically advanced, particularly when drawing parallels with realms like the BPO sector. Of course, this does not imply that workers receive relief from surveillance. Much to the contrary, the Indian garment sector has long been critiqued by civil society and trade unions for worker exploitation via excessive surveillance on the shop floor. Akin to the case of Amazon delivery workers feeling so pressurized as to be unable to take a restroom break, garment workers in India and several other countries face relentless supervision on the shop floor. This issue is inextricably linked with the pursuit of "productivity," with many types of garment factories requiring workers to produce a certain number of products per day in a desire to comply with factory production targets (Equal Times). In the garment industry, monitoring tools frequently include biometric fingerprint scanning for attendance records and CCTV monitoring for employee activity on the shop floor. Additionally, this renders the surveillance more "direct" than the case of the algorithmic cruelties to which, as observed in the preceding section, platform workers are frequently subjected. It is also key to note that in India, akin to other developing country hubs for garment manufacturing and exports, the shop floor tends to be a heavily gendered space (Business and Human Rights Resource Centre). This means that women are more likely to be employed in jobs such as stitching relative to their male counterparts.

Added to the above considerations in India's garment sector is the employment of "digital Taylorism," involving the slicing up of labour into minuscule tasks, enabling employers to keep an even closer check on workers' frequency and duration of rest breaks. Employers typically frame these mechanisms as "security measures" against theft and pilferage in the factory, yet again attempting to labour-wash surveillance efforts. While the garment industry currently deploys commonplace surveillance mechanisms, enclave economies (tea and coffee plantation workers), which earlier had a physical record-keeping system and supervisor-based surveillance, are now seeing a shift to surveillance as in the garment industry. In the case of India's tea and coffee plantation workers, trends in surveillance now

mean that factories may employ biometric attendance and facial recognition software to record worker activity. Companies in India, such as Softweb Technologies, are at the forefront of facial recognition systems, attempting to alter the face of employee monitoring in enclave economies (Softweb Solutions).

While the aforementioned examples cite surveillance endeavors by the private sector, the surveillance of workers stretches far beyond the realm of private industry alone. In India, several civic bodies have been reported as using technological surveillance methods to monitor staff and citizens. For instance, the Madurai Corporation employs facial recognition systems to monitor the attendance of sanitation workers, while the Panchkula Municipal Corporation requires sanitation workers to use “human efficiency trackers”- wearable hand gadgets that track their bodily movements (The Center for Internet and Society, 2023). Within the government ecosystem, the ASHA workers in Haryana have also reported the installation of an MDM (Mobile Device Management) 360 shield for worker tracking, which the workers alleged would jeopardize their digital privacy (Garg, 2021).

2) Conclusion: Protecting Worker Interests

The above analysis indicates that worker interests in India must be protected from employer surveillance on various levels, ranging from surveillance/monitoring being used as a tool for rights violations like stopping bathroom breaks; to the issue of invading worker privacy. The first level at which this must be considered is of course, that of legal protections in the workplace. The Right to Privacy is recognised as a fundamental right by the Supreme Court of India (Puttuswamy judgement, 2017), but it is not an absolute right, which implies that it comes with limitations, especially when it pertains to public interest. (Bhandari, Joshi, and Sahai, 2017).

The incoming Digital Personal Data Protection Act (DPDPA) 2023, slated to replace the existing IT Act of 2000, provides some information safeguards through the clauses of informed consent and freedom of consent withdrawal. The DPDPA, however, does permit the collection of ‘personal’ data for “certain legitimate uses” that are not clearly defined under the law, thus proffering companies some leeway to define “legitimate use” and leaving vast room for employers to pry into the personal data of workers. An important concern is that the DPDPA should differentiate between personal identifiable data and “sensitive data” to safeguard the citizenry against unethical data collection by employers. While in India, customers have the absolute right to withdraw consent, employees are not under the category, and as discussed earlier in this paper, given the power imbalances between employers and workers, the latter are routinely forced to consent to information-sharing (Mohandas and Srinvasa, 2020). One recent example of an excessive intrusion of worker privacy has been Tech Mahindra’s shift to use facial recognition devices to check the mood of the workforce. For best practice examples in terms of data privacy, a good place to look would be the EU and UK’s General Data Protection Regulations (GDPR), a landmark data protection law, which defines sensitive data as “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person’s sex life or sexual orientation,” and prohibits employers from collecting such information.

The safeguarding of workers' privacy in the workplace must also be read in line with other labour protections for workers. For example, whether or not technology is the means to restrict the bathroom breaks of workers, this restriction is itself counter to India's labour laws. Another fundamental way in which worker rights can be ensured is by ensuring that workers are allowed the right to unionize. Most, there seems to be a close overlap between the deployment of different types of surveillance and the desire of employers to restrict workers' organizing freedoms. This is apparent from examples such as the BPO industry and the tech sector at large, where the word "union" is often considered in a very poor light by employers (Raju, 2023). The predicament of workers in industries such as the tech sector and the ICT industry on the whole calls into question whether India has indeed moved past the model of the "electronic sweatshop," as some have argued. This is true in the Indian context. However, worker organizing has become common in electronic spaces, with workers also utilizing digital tools as a form of conveyance to empowerment (Poster, 2011).

The path to ensuring worker interests are safeguarded in the workplace is a long and tricky one given the imbalance of power between workers and employers in an era of "surveillance capitalism." It remains important to stay steadfast to this path, despite these difficulties, and unionisation remains one key and proven way in which imbalances in power can be checked.

References

Amnesty International. "What Is Big Tech's Surveillance-Based Business Model?" Amnesty International, February 2022. Accessed June 5, 2024. <https://www.amnesty.org/en/latest/campaigns/2022/02/what-is-big-techs-surveillance-based-business-model/>.

Athreya, Bama. "Slaves to Technology: Worker control in the surveillance economy." *Anti-Trafficking Review* 15 (2020): 82-101.

Bhandari, A. K., Joshi, A. P., & Sahai, A. (2017). "An Analysis of Puttaswamy: The Constitutionality of Aadhaar." Accessed June 6, 2024. https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1.

Bhavan, T. and Bhavan, V. P. O. (2020) 'Interstate migrant workers in Kerala; a study on their work and life.'

Business & Human Rights Resource Centre. "India: Garment Worker Allegedly Raped, Murdered by Supervisor at H&M Supplier Natchi Apparels After Months of Sexual Abuse, Harassment (incl. H&M's response)." Accessed June 6, 2024. <https://www.business-humanrights.org/en/latest-news/india-garment-worker-allegedly-raped-murdered-by-supervisor-at-hm-supplier-natchi-apparels-after-months-of-sexual-abuse-harassment-incl-hms-response/#:~:text=On%20%20January%202021%2C%20Jeyasre,Indian%20media%20as%20V%20Thangadurai>.

Clavell, G. G. (2011) 'The political economy of surveillance in the (Wannabe) global city,' *Surveillance and Society*, 8(4), pp. 523–526. doi: 10.24908/ss.v8i4.4191.

Eckstein, I. and Mawii, Z. (2020) *Workplace Monitoring: Data collection practices and emerging risks for low wage workers in India*.

EmpMonitor. "User Activity Monitoring." EmpMonitor. Accessed June 6, 2024. <https://empmonitor.com/user-activity-monitoring/>.

Eurofound (2020) *Employee monitoring and surveillance: The challenges of digitalisation*, Publications Office of the European Union. doi: 10.2806/424580.

Equal Times. "India's Garment Workers Continue to Face Exploitation Despite Global Brands' Promises." Accessed June 6, 2024. <https://www.equaltimes.org/india-s-garment-workers-continue?lang=en>.

Garg, R. (2021) # PrivacyofThePeople - ASHA Workers and Employee Surveillance In our new series # PrivacyofThePeople , we will look at the impact of the Personal Data Protection Bill , 2019 on different sections of society . In this post , we discuss how the Bill affects, Internet Freedom Foundation. Available at: <https://internetfreedom.in/privacyofthepeople-asha-workers-and-employee-surveillance/>.

Gray, Mary L., and Siddharth Suri. *Ghost work: How to stop Silicon Valley from building a new global underclass*. Eamon Dolan Books, 2019.

Harper, Jon. "Surveillance State: How Big Tech Powers and Profits from Your Data." *The Intercept*, October 16, 2023. Accessed June 5, 2024.
<https://theintercept.com/2023/10/16/surveillance-state-big-tech/>.

Internet Freedom Foundation. "Privacy of the People: ASHA Workers and Employee Surveillance." Accessed June 6, 2024. <https://internetfreedom.in/privacyofthepeople-asha-workers-and-employee-surveillance/>.

Mateescu, A. and Nguyen, A. (2019) 'Explainer: Workplace Monitoring & Surveillance,' Data & Society Research Institute, (February), pp. 1–17. Available at: www.datasociety.net. Mohandas, Shweta, and Deepika Nagagudi Srinivasa. "The Boss Will See You Now - the Growth of Workplace Surveillance in India, Is Data Protection Legislation the Answer?" Centre for Internet & Society, December 31, 2020. <https://cis-india.org/internet-governance/blog/the-boss-will-see-you-now-the-growth-of-workplace-surveillance-in-india-is-data-protection-legislation-the-answer>.

Munich Business School. "Taylorism." Accessed June 6, 2024. <https://www.munich-business-school.de/en/l/business-studies-dictionary/taylorism#:~:text=Taylorism%2C%20named%20after%20the%20American,reduce%20costs%20and%20increase%20quality>.

Mukherjee, Piu; Bino, Paul G D; Pathan, J. I. (2013) 'Migrant Workers in Informal Sector : A Probe into Working Conditions,' ATLMRI Discussion Paper Series, p. 30.

National Campaign on Dalit Human Rights. *India Report*. July 2023. Accessed June 6, 2024. https://www.ncdhr.org.in/wp-content/uploads/2023/07/India-Report_new-1.pdf.

Poster, Winifred R. "Emotion detectors, answering machines, and e-unions: Multi-surveillances in the global interactive service industry." *American Behavioral Scientist* 55, no. 7 (2011): 868-901.

Prasad-Aleyamma, M. (2018) 'Cards and carriers: migration, identification, and surveillance in Kerala, South India,' *Contemporary South Asia*, 26(2), pp. 191–205. doi: 10.1080/09584935.2017.1407293.

Raju, Namrata. "Ensuring Job Security and Workers' Rights in India's Tech Sector." *The News Minute*, Accessed July 5, 2024. <https://www.thenewsminute.com/news/ensuring-job-security-and-workers-rights-india-s-tech-sector-177067>.

Sahu, A. (2023) *Boss is watching : More takers for tools to monitor employees*, Money Control. Available at: <https://www.moneycontrol.com/news/business/employee-monitoring-tools-see-strong-demand-post-pandemic-11488471.html>.

Sahni, Kriti. "How Women Are Increasingly Affected by Surveillance Culture." *Feminism in India*, July 19, 2023. Accessed June 6, 2024. <https://feminisminindia.com/2023/07/19/how-women-are-increasingly-affected-by-surveillance-culture/>.

Sardar, Zofeen Ebrahim. "We Are Watching: The Rising Tide of Digital Surveillance." *New Internationalist*, February 13, 2023. Accessed June 6, 2024. <https://newint.org/features/2023/02/13/your-watch>.

Softweb Solutions. "Face Recognition Attendance for Agri-Plantation Industry." Accessed June 6, 2024. <https://softweb.co.in/blog/face-recognition-attendance-for-agri-plantation-industry/>.

Sinha, A. (2024) 'The Landscape of Facial Recognition Technologies in India,' TechPolicy.Press, pp. 1–9. Available at: <https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/>.

T, A. (2023) 'Kerala government mulls on Police clearance from home state for migrant workers', *The New Indian Express*, pp. 8–11.

The Center for Internet and Society (2023) *The Boss Will See You Now - The Growth of Workplace Surveillance in India, is Data Protection Legislation the Answer?* Available at: <https://cis-india.org/internet-governance/blog/the-boss-will-see-you-now-the-growth-of-workplace-surveillance-in-india-is-data-protection-legislation-the-answer>.

UNIGlobal. (2021). *The Amazon Panopticon: A Guide for Workers, Organisers and Policymakers*. UNIGlobal Union.

Zuboff, Shoshana. "The age of surveillance capitalism." In *Social theory re-wired*, pp. 203-213. Routledge, 2023.

ⁱ UNIGlobal. (2021). *The Amazon Panopticon: A Guide for Workers, Organisers and Policymakers*. UNIGlobal Union.

ⁱⁱ The 'informal sector' in India is defined as "The unorganized sector consists of all unincorporated private enterprises owned by individuals or households engaged in the sale and production of goods and services operated on a proprietary or partnership basis and with less than ten total workers." (National Commission for Enterprises in the Unorganised Sector)

ⁱⁱⁱ ASHA is an acronym for Accredited Social Health Activist. An ASHA worker is a community-level worker functioning as a health care facilitator, and a service provider and to generate awareness on health-related issues.